

RECEIVED
CENTRAL FAX CENTER

Appl. No.: 09/944,694
Amdt. dated February 28, 2007
Reply to Official Action of September 28, 2006

FEB 28 2007

REMARKS/ARGUMENTS

This Reply is filed in response to the new, non-final Official Action of September 28, 2007, the Official Action being issued following a Notice of Panel Decision from Pre-Appeal Brief Review re-opening prosecution of the present application. The new, non-final Official Action no longer rejects all of the pending claims, namely Claims 1-18, under 35 U.S.C. § 102(e) as being anticipated by U.S. Patent No. 6,775,772 to Binding et al.; or rejects any of the claims under 35 U.S.C. § 112, first paragraph. Instead, the Official Action now rejects Claims 3 and 12-18 as being anticipated by Binding; and rejects the remaining claims, namely Claims 1, 2 and 4-11, under 35 U.S.C. § 103(a) as being unpatentable over newly-cited U.S. Patent No. 7,032,242 to Grabelsky et al., in view of newly-cited U.S. Patent No. 6,356,529 to Zarom. As explained below, Applicant respectfully submits that the claimed invention is patentably distinct from Binding, Grabelsky and Zarom, and that at least Grabelsky and Zarom cannot reasonably be combined to disclose the claimed invention. Accordingly, Applicant traverses the rejections of the claims as being anticipated by Binding, or as being unpatentable over Grabelsky in view of Zarom. In view of the remarks presented herein, Applicant respectfully requests reconsideration and allowance of all of the pending claims of the present application.

A. Claims 3 and 12-18

The new, non-final Official Action rejects Claims 3 and 12-18 as being anticipated by Binding. As background, Binding discloses a piggy-backed key exchange protocol for providing low-overhead browser connections from a client to a server using a trusted third party. According to one disclosed scenario implementing the disclosed system, a client sends the server a common HTTP message (e.g., HTTP GET) that includes security-sensitive parameters encrypted using scheme M1 (i.e., parameters \rightarrow M1[parameters]). The server, being unable to process the encrypted parameters, encrypts the encrypted parameters using scheme M2 (i.e., M1[parameters] \rightarrow M2[M1[parameters]]), and forwards the further-encrypted parameters to a trusted third party (TTP). Being configured to process messages encrypted with either scheme M1 or scheme M2, the TTP decrypts the further-encrypted parameters using scheme M2 (i.e., M2[M1[parameters]] \rightarrow M1[parameters]), and then decrypts the encrypted parameters using

Appl. No.: 09/944,694
Amtd. dated February 28, 2007
Reply to Official Action of September 28, 2006

scheme M1 (i.e., $M1[\text{parameters}] \rightarrow \text{parameters}$), the decryption steps resulting in cleartext parameters (i.e., parameters). Thereafter, the TTP re-encrypts the cleartext parameters using scheme M2 (i.e., $\text{parameters} \rightarrow M2[\text{parameters}]$), and forwards the re-encrypted parameters to the server. The server decrypts the re-encrypted parameters using scheme M2 to similarly obtain the cleartext parameters (i.e., $M2[\text{parameters}] \rightarrow \text{parameters}$).

According to a first aspect of the claimed invention, as reflected by independent Claim 3, a system for providing network security includes means for receiving a request to perform a cryptographic operation, and means for returning a response to the cryptographic operation request. In addition, the system also includes means for translating a first plurality of cleartext data into a second plurality of cleartext data in accordance with one or more translation rules. Further, the system includes one or more modules for performing the cryptographic operations, including obtaining the first plurality of cleartext data based upon a first plurality of encrypted data, and encrypting the second plurality of cleartext data to obtain a second plurality of encrypted data.

As explained in response to the final Official Action and in the Pre-Appeal Brief Request For Review (from which the Notice of Panel Decision issued), in contrast to the first claimed invention, Binding does not teach or suggest translating a first plurality of cleartext data (e.g., associated with WML) into a second plurality of cleartext data (e.g., associated with HTML) in accordance with at least one translation rule. Instead, Binding discloses a number of steps whereby security-sensitive parameters are encrypted and decrypted to transfer those parameters between a client and server. In accordance with Binding, however, the only cleartext data is the parameters, which are nowhere translated from one form to another (noting that the term "translating" is well understood to those skilled in the art as meaning to change from one form to another).

In response to the foregoing, the new, non-final Official Action alleges that Binding discloses decrypting a message (citing col. 15, line 37), and then performing a second decryption of that message (citing col. 15, lines 38-39). The Official Action then alleges that the second decryption corresponds to the recited translation of first plurality of cleartext data into a second plurality of cleartext data. As more particularly disclosed at the cited passages of Binding, a TTP

Appl. No.: 09/944,694
Amdt. dated February 28, 2007
Reply to Official Action of September 28, 2006

receives security-sensitive parameters encrypted using scheme M1, the resulting encoded parameters itself then being further encrypted using scheme M2, resulting in the following: $M2[M1[\text{parameters}]]$. As indicated above, the TTP decrypts the further-encrypted parameters using scheme M2 (i.e., $M2[M1[\text{parameters}]] \rightarrow M1[\text{parameters}]$), and then decrypts the encrypted parameters using scheme M1 (i.e., $M1[\text{parameters}] \rightarrow \text{parameters}$), the decryption steps resulting in cleartext parameters (i.e., parameters).

The Official Action appears to allege that the decrypting operation $M1[\text{parameters}] \rightarrow \text{parameters}$ corresponds to the recited translation of a first plurality of cleartext data into a second plurality of cleartext data. As readily seen, however, $M1[\text{parameters}]$ is not cleartext data. In this regard, cleartext data is well known to those skilled in the art as data without cryptographic protection. See Wikipedia, *Cleartext – Wikipedia, the Free Encyclopedia* (last modified Dec. 18, 2006) <<http://en.wikipedia.org/wiki/Cleartext>> (explaining that “cleartext is the form of a message or data which is transferred or stored without cryptographic protection” – emphasis added). The Official Action may interpret the encrypted parameters $M1[\text{parameters}]$ as cleartext data since the encrypted parameters themselves are not further encrypted (using scheme M2). This interpretation, however, is not only inconsistent with the plain meaning of the term “cleartext,” but also inconsistent with the interpretation one skilled in the art would give the term. See MPEP § 2111.

Applicant therefore respectfully submits that independent Claim 3, and by dependency Claims 12-18, is patentably distinct from the system and method of Binding. As such, Applicant respectfully submits that the rejection of Claims 3 and 12-18 as being anticipated by Binding is overcome.

B. Claims 1, 2 and 4-11

The Official Action also rejects Claims 1, 2 and 4-11 as being unpatentable over Grabelsky in view of Zarom. Newly-cited Grabelsky discloses a system and method for distributed network address translation with security features provided by Internet Protocol security protocol (“IPsec”). The distributed network address translation is accomplished with IPsec by mapping a local Internet Protocol (IP) address of a given local network device and a

Appl. No.: 09/944,694
Amdt. dated February 28, 2007
Reply to Official Action of September 28, 2006

IPsec Security Parameter Index ("SPI") associated with an inbound IPsec Security Association ("SA") that terminates at the local network device. In a passage of Grabelsky cited in the Official Action, IPsec defines the security service Encapsulated Security Payload (ESP), and may be applied in a transport mode. In the transport mode, a sending endpoint may apply ESP to outbound packets in a manner including encapsulating information using a selected encryption technique (col. 23, ll. 27-39). Separately, a receiving endpoint may apply ESP to inbound packets in a manner including decryption using an encryption technique indicated by an appropriate security association (SA) (col. 23, l. 49 – col. 24, l. 4).

Newly-cited Zarom discloses a system and method for translating between data transmitted according to the WAP network protocols and data transmitted according to IP protocols. As disclosed, wireless communication devices that operate in accordance with WAP network protocols require a translation system, or gateway, to communicate with other devices that operate in accordance with IP protocols. Zarom therefore discloses a system and method for WAP translation in a manner that enables a gateway translator to perform the translation process as soon as a minimal portion of data has been received.

According to a second aspect of the claimed invention, as reflected by independent Claim 1, a method for providing network security includes receiving a plurality of network protocol packets (e.g., IP packets). A network protocol packet includes a network protocol header (e.g., IP header) and a plurality of network protocol data, which includes a first cryptographic protocol header (e.g., TCP header) and a first plurality of encrypted data (e.g., SSL data). At least a portion of some of the network protocol packets are configured in accordance with a transport layer protocol (e.g., TCP/UDP) or a network layer protocol (e.g., IP). As also recited, a first plurality of cryptographic protocol rules (e.g., WTLS rules) associated with the network protocol data is determined, with a cryptographic session being established if required by the first cryptographic rules. The first plurality of cryptographic protocol rules are applied to the first encrypted data to obtain a first plurality of cleartext data (e.g., WML data). The first plurality of cleartext data is translated into a second plurality of cleartext data (e.g., HTML data) in accordance with at least one translation rule. The second plurality of cleartext data is then encrypted in accordance with at least one rule associated with a second cryptographic protocol

Appl. No.: 09/944,694
Amdt. dated February 28, 2007
Reply to Official Action of September 28, 2006

(e.g., HTTP over SSL), resulting in a second plurality of encrypted data.

In contrast to the second aspect of the claimed invention, and as conceded in the Official Action, Grabelsky does not teach or suggest translating a first plurality of cleartext data into a second plurality of cleartext data. Nonetheless, the Official Action alleges that Zarom discloses this feature, and that one skilled in the art would have been motivated to modify Grabelsky to include the aforementioned feature of Zarom to teach the claimed invention. Applicant disagrees, and respectfully submits that, even if Grabelsky and Zarom did disclose respective features of the claimed invention, one skilled in the art would not in fact have been motivated to modify Grabelsky to include the feature of Zarom to teach the claimed invention.

Initially, Applicant notes that the Official Action cites a passage of Grabelsky directed to a receiving endpoint applying ESP to inbound packets, and alleges that this passage reads on the claimed feature of applying a first plurality of cryptographic protocol rules to first encrypted data to obtain a first plurality of cleartext data. The Official Action cites a passage of Grabelsky directed to a sending endpoint applying ESP to outbound packets, and alleges that this passage reads on the claimed feature of encrypting a second plurality of cleartext data into a second plurality of encrypted data. Then, the Official Action cites Zarom for disclosing a gateway translator translating between data transmitted according to the WAP network protocols and data transmitted according to IP protocols, and alleges that this passage reads on the intervening translation of the first plurality of cleartext data into the second plurality of cleartext data.

Taking the Official Action's interpretation of Grabelsky and Zarom as a given (although expressly not admitted), one could argue that the combination of Grabelsky and Zarom teaches a receiving endpoint decrypting first encrypted data into a first plurality of cleartext data, a gateway translator then translating the first plurality of cleartext data into a second plurality of cleartext data, followed by a sending endpoint encrypting the second plurality of cleartext data into a second plurality of encrypted data (although, again, expressly not admitted). To effectuate the security services of Grabelsky, it only makes logical sense that the functions attributed to the receiving endpoint, gateway translator and sending endpoint are all performed by a single entity between endpoints within different networks (and thus needing address translation), such as by the router of Grabelsky. As disclosed by Grabelsky, however, the router does not modify the

Appl. No.: 09/944,694
Amdt. dated February 28, 2007
Reply to Official Action of September 28, 2006

contents of received, secured (IPsec) packets since to do so would compromise the security of those packets. See Grabelsky, col. 3, l. 54 – col. 4, l. 3; col. 25, ll. 31-34; Col. 32, ll. 45-46. Thus, even given the Official Action's interpretation of Grabelsky and Zarom (again expressly not admitted) one skilled in the art would not be motivated to modify the end-to-end address translation with security of Grabelsky, with the translation of Zarom, to disclose the claimed invention.

Applicant therefore respectfully submits that independent Claim 1, and by dependency Claims 4-11, is patentably distinct from Grabelsky and Zarom, taken individually; and respectfully submit that Grabelsky and Zarom cannot reasonably be combined to teach or suggest independent Claim 1, and by dependency Claims 4-11. Applicant also respectfully submits that independent Claim 2 recites subject matter similar to that of independent Claim 1. As such, Applicant respectfully submits that independent Claim 2 is patentably distinct from Grabelsky and Zarom for at least those reasons explained above with respect to independent Claim 1.

1. Dependent Claims 6 and 9

In addition to the aforementioned reasons, Applicant respectfully submits that various ones of dependent Claims 4-11 recite features that are further patentably distinct from Binding, Grabelsky and Zarom, taken individually or in combination. For example, dependent Claims 6 and 9 further recite that the first and second cryptographic protocols comprise WTLS and SSL over HTTP, respectively. The Official Action cites Zarom for allegedly disclosing the features of Claims 6 and 9, citing column 3, lines 5-6 for disclosing WTLS, and citing column 8, lines 7-11 for disclosing SSL over HTTP. Applicant respectfully submits, however, that not only do neither of these passages disclose the features to which they are attributed, but no other passage of Zarom disclose those features.

For at least the foregoing reasons, Applicant respectfully submits that the rejection of Claims 1, 2 and 4-11 as being unpatentable over Grabelsky, in view of Zarom, is overcome.

Appl. No.: 09/944,694
Amdt. dated February 28, 2007
Reply to Official Action of September 28, 2006

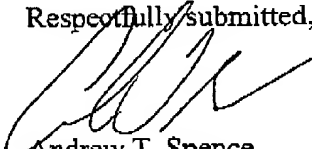
RECEIVED
CENTRAL FAX CENTER
FEB 28 2007

CONCLUSION

In view of the remarks presented above, Applicant respectfully submits that the present application is in condition for allowance. The issuance of a Notice of Allowance is therefore respectfully requested. In order to expedite the examination of the present application, the Examiner is encouraged to contact Applicant's undersigned attorney in order to resolve any remaining issues.

It is not believed that extensions of time or fees for net addition of claims are required, beyond those that may otherwise be provided for in documents accompanying this paper. However, in the event that additional extensions of time are necessary to allow consideration of this paper, such extensions are hereby petitioned under 37 CFR § 1.136(a), and any fee required therefore (including fees for net addition of claims) is hereby authorized to be charged to Deposit Account No. 16-0605.

Respectfully submitted,

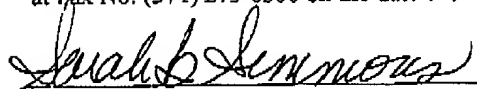


Andrew T. Spence
Registration No. 45,699

Customer No. 00826
ALSTON & BIRD LLP
Bank of America Plaza
101 South Tryon Street, Suite 4000
Charlotte, NC 28280-4000
Tel Charlotte Office (704) 444-1000
Fax Charlotte Office (704) 444-1111

CERTIFICATION OF FACSIMILE TRANSMISSION

I hereby certify that this paper is being facsimile transmitted to the US Patent and Trademark Office at fax No. (571) 273-8300 on the date shown below.



Sarah B. Simmons

February 28, 2007
Date

LE:AL02/30274530v1

8 of 8